UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES

CARRERA DE DERECHO

"EL FRAUDE COMO DELITO INFORMÁTICO"

Autora:

Ana Maribel Chungata Cabrera

Director:

Dr. Juan Antonio Peña Aguirre

Monografía previa a la obtención del Título de "*Abogado de los Tribunales de Justicia de la República del Ecuador y Licenciado en Ciencias Políticas y Sociales"*

Cuenca, Ecuador

Marzo 2015

Resumen

La necesidad del hombre de descubrir cada día más y su necesidad de invención lo ha llevado a la creación de la tecnología como mecanismo de evolución, en donde la sociedad no se detiene y cada día espera algo nuevo. Sin embargo, esta evolución ha traído consecuencias nefastas, porque los ciberdelincuentes han utilizado la informática como medio idóneo para cometer hechos ilícitos en la sociedad de la información.

Es por ello, que el presente trabajo trata acerca de los orígenes de la informática y los delitos informáticos, los tipos de delitos informáticos más comunes en el medio. Siendo el Fraude Informático, delito a analizarse, sus modalidades, la tipificación penal dentro de la legislación ecuatoriana, española y argentina, finalmente se establece recomendaciones para evitar ser víctima de un delito informático.

Palabras Claves: Fraude Informático, delitos informáticos, fraude informático en la legislación ecuatoriana, el fraude informático en el COIP.

Abstract

Man's need to discover every day and their need for invention has led to the creation of technology as a mechanism of evolution, where the society does not stop and expect something new every day. However, this evolution has brought dire consequences because cybercriminals have used the computer as a suitable means of committing wrongful acts in the information society.

That is why, the present work discusses about origins of computer and cybercrime, the most common types of cybercrime in the society. Being the Computer Fraud, the crime will be analyzed, its modalities, criminal typification within Ecuador legislation, Spain legislation and Argentina legislation, finally give recommendations to avoid becoming a victim of computer crime.

Key words: Computer fraud, computer crime, computer fraud in Ecuadorian law, computer fraud in the COIP.

INDICE

UNIVERSIDAD DE CUENCA
FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES
ESCUELA DE DERECHO

Cláusula de derechos de autor

Yo, Ana Maribel Chungata Cabrera, autora de la monografía "EL FRAUDE COMO DELITO INFORMÁTICO", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de "Abogado de los Tribunales de Justicia de la República del Ecuador y Licenciado en Ciencias Políticas y Sociales". El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autora

Cuenca, marzo de 2015

Ana Maribel Chungata Cabrera

C.I: 0105304240

Ana Maribel Chungata Cabrera

UNIVERSIDAD DE CUENCA
FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES
ESCUELA DE DERECHO

Cláusula de propiedad intelectual

Yo, Ana Maribel Chungata Cabrera, autora de la monografía "EL FRAUDE COMO DELITO INFORMÁTICO", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, marzo de 2014

Ana Maribel Chungata Cabrera

C.I: 0105304240

Ana Maribel Chungata Cabrera

Dedicatoria

Con mucho cariño a mis padres quienes me apoyaron arduamente en este largo trayecto y siempre confiaron en mí, convirtiéndose en el pilar fundamental de mi vida profesional. Y de manera especial, con mucho amor a mi sobrina.

Anita

Agradecimiento

A los señores profesores de la Escuela de Derecho de la Facultad de Jurisprudencia de la distinguida Universidad de Cuenca, por haberme impartido sus conocimientos durante los 5 años de carrera de formación y principalmente mi más sincero agradecimiento al Dr. Juan Peña Aguirre, quien dirigió el presente trabajo brindándome sus conocimientos y apoyo para la culminación del mismo.

Anita

INTRODUCCIÓN

El Derecho está en constante cambio, es dinámico, por lo que si la sociedad se desarrolla el derecho también. Dicho progreso ha sido posible en gran parte por la tecnología e informática, que en el transcurso de la historia ha cambiado de generación en generación para ayudar al ser humano en sus distintas actividades como puede ir desde cuestiones laborales, estudiantiles hasta el ocio.

Es por ello que se ha visto la imperiosa necesidad de innovar, crear una nueva ciencia jurídica, de acorde a la época tecnológica, como es el derecho informático, ciencia autónoma del derecho especializada en el tema de la informática, usos, aplicaciones e implicaciones legales. Sin embargo, no puede ser tratada de una manera aislada, pues está relacionada con las demás ciencias jurídicas como el derecho penal, derecho civil y derecho comercial.

El derecho informático trata acerca de la sociedad de la información y a su vez la sociedad de la información implica la tecnología de la información y comunicaciones, que crea plataformas para el tránsito de ideas, información, comunicación en el mundo, siempre con el internet como herramienta fundamental en la tecnología.

Pero en dicha sociedad de la información empiezan a cometerse hechos ilícitos por parte de los denominados ciberdelincuentes que buscan desestabilizar la armonía en la que se encuentra la colectividad, estos hechos son los denominados Delitos Informáticos y dentro de estos se puede mencionar algunos de los más importantes como el Fraude Informático, el sabotaje informático, el terrorismo informático entre otros, constituyéndose algunos de la extensa posibilidades de delitos contra la tecnología que existen.

Ante lo cual el presente trabajo investigativo trata de manera general los delitos informáticos, sus clases, en especial lo relacionado al Fraude Informático, sus modalidades y la regulación respectiva dentro de la legislación ecuatoriana a fin de combatir la criminalidad informática con respecto al fraude.

CAPÍTULO I: GENERALIDADES

Al tratar del tema de la globalización, imperantemente pensamos en el avance tecnológico que ha ido progresando por el paso del tiempo hasta la actualidad, en la que, no podemos concebir un normal desarrollo de una sociedad sin la ayuda de la tecnología, del internet y los aparatos electrónicos en general. Sin embargo, todo progreso lamentablemente se ve empañado de actividades que en vez de ayudar perjudican a la sociedad, y dentro del ámbito de la informática y avance tecnológico, hemos de tratar sobre los denominados Delitos Informáticos y a su vez específicamente del Fraude Informático, que hoy en día en el Ecuador vemos que se ha ido incrementando, y lo vemos en una publicación del Diario El Telégrafo con fecha 17 de septiembre de 2012, como reseña, que nos dice "*Desde el 2009 el aumento de denuncias es dramático, en ese año se reportaron solamente 168 casos, mientras que en lo que va de 2012 llegan a 1.564*", haciendo referencia a las denuncias por fraude informático y que el sector bancario es el blanco de este tipo de delitos, en donde el objetivo para el criminal informático es el dinero de los cuenta ahorristas de estas entidades, que por medios fraudulentos se apropian de su dinero.

A más de esto, tal como lo publica diario El Comercio en su portal web el 19 de septiembre de 2014, "*Los anuncios se difunden de forma masiva en las páginas de Internet, en Ecuador. Los 'hackers' ofrecen obtener las claves de Hotmail, Yahoo, Gmail o Facebook. Afirman que las operaciones son 100% "garantizadas*", *porque las víctimas no se percatan de la profanación*". Este tipo de conductas criminales, pone bajo alerta a la sociedad en general, ya que cualquier persona podría ser víctima de este delito informático.

Con estas consideraciones, con la finalidad de analizar algunos delitos informáticos y sobretodo el Fraude Informático, los mecanismos legales para enfrentarlos y el impacto en la sociedad, es menester partir desde el

origen de la informática, con miras a la mejor comprensión del fenómeno tecnológico.

1.1 Antecedentes: El Derecho Informático

Para abordar el tema del derecho informático hay que hacer una breve referencia a la historia de la informática.

La informática y sus generaciones

El origen más remoto de la computadora se encuentra en el año 3.000 a. c., en las antiguas civilizaciones como la de Babilonia en donde se originó el primer invento mecánico de contabilidad que fue el Abaco que servía para realizar cálculos de adición y sustracción.

Luego un hecho importante dentro de la historia de la informática se produce en el siglo XVII con la invención de la maquina calculadora del científico francés Blaise Pascal denominada *roue pascaline* (rueda de pascal) o Pascalina, que en un inicio solo realizaba sumas, pero con el transcurso de los años Pascal lo mejoro pudiendo así realizar sumas y restas. Posteriormente el filósofo, lógico, matemático y jurista alemán Gottfried Wilhelm Leibniz, ya en el siglo XVIII, toma la pascalina como base y desarrolla una maquina capaz de realizar operaciones de adición, sustracción, multiplicación, división y cociente.

Así en el siglo XIX se comercializaría las primeras máquinas de calcular. Pero es en este mismo siglo que el matemático británico y científico de la computación Charles Babbage diseñó la máquina analítica para ejecutar programas de tabulación o computación, que disponía de una memoria que podía almacenar 1000 números de 50 cifras. Previamente siendo el primer intento la máquina diferencial, que fue un computador diseñado para realizar actividades específicas como realizar cálculos, almacenar y seleccionar información, resolver problemas y entregar resultados impresos, sin embargo nunca llego a realizarse talvez por las limitaciones

tecnológicas de la época que eran un obstáculo para su construcción sin embargo estos diseños le sirvió para ser considerado dentro de la historia como el precursor de la computadora.

En esta misma época Augusta Ada Byron matemática británica ayudó con el desarrollo del diseño de la maquina diferencial de Babbage creando programas para la misma, desarrollando el primer lenguaje de software denominado ADA, diseñó el primer algoritmo[1] destinado a ser procesado por una máquina, por lo que fue reconocida como la primera programadora de ordenadores en la historia de la informática.

Pero todas estas máquinas hasta entonces tenían un problema y es que eran mecánicas, razón por la cual en el siglo XX paralelamente con el desarrollo de la electrónica, se empieza a solucionar estos problemas de las máquinas reemplazando así los sistemas de engranaje y varillas por impulsos eléctricos, estableciendo que cuando hay un paso de corriente eléctrica será representado con el 1 y cuando no, se representara con un 0, originándose así el sistema binario, fundamento virtualmente de todas las arquitecturas de las computadoras actuales, es un sistema de numeración en los que se utilizan como ya se mencionó las cifras uno y cero, esto debido a que las computadoras trabajan internamente con dos niveles de voltaje siendo encendido 1 y apagado 0.

En la década de 1880 el estadístico estadounidense Herman Hollerith, logró el tratamiento automático de la información, de donde nace el término "informática"[2], resultado de utilizar tarjetas perforadas para procesar datos, que eran una tarjeta en donde los datos se señalaban haciendo un agujero que luego serían leídos por un dispositivo electromecánico denominado la maquina tabuladora, en el censo poblacional realizado en el año de 1890 de Estados Unidos, lo novedoso fue que los datos de 60 millones de

[1] Grupo finito de operaciones organizadas de manera lógica y ordenada que permite solucionar un determinado problema. Se trata de una serie de instrucciones o reglas establecidas que, por medio de una sucesión de pasos, permiten arribar a un resultado o solución.

[2] Información automática

ciudadanos se procesaron en menos de tres años, que ha comparación de anteriores censos no se llegaba a procesar los datos hasta el siguiente censo que se realizaba cada diez años. A partir de esto Holeerith diseño nuevas máquinas y en el año de 1896 fundo la IBM, una de las compañías más importantes en la industria de la informática luego de la segunda guerra mundial.

Durante la segunda guerra mundial se construyeron computadoras con propósitos militares por ejemplo la Z3 fue construida por los alemanes para codificar mensajes, o los ingleses que construyeron el Colossus, siendo computadoras que poseían dimensiones gigantescas.

Desde aquí empieza la generación de las computadoras, siendo las siguientes:

Primera Generación

Desde 1940 a 1952, las computadoras de esta generación utilizaban bulbos[3] o tubos vacíos para procesar información, estas computadoras eran más grandes y generaban más calor que los modelos actuales.

Dentro de esta generación se encuentra:

- La primera computadora electromecánica denominada Mark.
- La UNIVAC I, la primera computadora comercial, que se lo utilizo para evaluar el censo de 1950.

Se programaban en lenguaje de máquina o lenguajes de programación que es un conjunto de instrucciones para que el ordenador efectúe una tarea, se denomina lenguaje de maquina porque debe escribirse mediante un conjunto de códigos binarios.

[3] Componente que se utiliza para amplificar, conmutar o modificar una señal eléctrica.

- Una versión mejorada de la UNIVAC I, fue la UNIVAC II, poseía una memoria de 2.000 a 10. 0000 palabras, utilizaba transistores y tubos de vacio.

Segunda Generación

Desde 1952 a 1954, lo que caracteriza esencialmente esta generación es el TRANSISTOR, que sustituyó los bulbos o tubos de vacio, siendo la IBM que lanzo un ordenador que empezó a utilizar la cinta magnética.

Además se crea el procesador de texto, el Word, las hojas de cálculo, el software pasa a tener un papel más importante que el hardware, y se destaca el código ASCII.

Tercera Generación

Desde 1954 a 1971, se destaca esta generación por el desarrollo del circuito integrado o microchip, los discos duros magnéticos, sistemas operativos con el Unix y el lenguaje de programación denominado Pascal, siendo el primero utilizado para programación, hoy en día se lo sigue utilizado para fines didácticos y aprendizaje. Gracias a los microchips las computadoras se hicieron pequeñas, más rápidas y eran energéticamente más eficaces que las anteriores.

Cuarta Generación

Desde 1971 a 1981, ya aparece el microprocesador de computadoras personales y el floppy disk conocido como el disquete. Estos microprocesadores significaban gran adelanto de la microelectrónica, siendo circuitos integrados de alta densidad y con gran velocidad. Dando nacimiento a la llamada “revolución informática”.

Quinta Generación

Desde 1982 en adelante, aparece el disquete de 3.5 pulgadas, protocolo TC/IP programas de Lotus 1,2,3, lenguajes de programación de alto nivel, microprocesadores como Pentium, tecnología Laser, sistemas operativos de alto nivel, aparece ya el Internet[4] junto con esta la tecnología Wifi[5].

La característica fundamental de esta generación es la innovación, la evolución de los ordenadores que ocupaban en sus inicios demasiado espacio a microcomputadores denominadas pc[6] y las supercomputadoras

Con el desarrollo de la sociedad, la industria, el área tecnológico va desarrollándose paulatinamente tanto en el software como en el hardware de los ordenadores, haciendo posible el acceso a las nuevas tecnologías diariamente al mayor número posible de usuarios que se ha convertido en una herramienta fundamental en la vida diaria de las personas y empresas.

Por esto como asevera el autor Téllez Valdez, *es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre (y no por la maquina como algunos pudieran suponer) encuentra sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es ilógico pensar que de no existir las computadoras, estas acciones no existirían*[7].

1.1.1 Criminalidad Informática

La criminalidad informática en la actualidad se orienta a los actos económicos criminales mediante la utilización de ordenadores o tecnologías de última generación, por lo que conceptualizando la

[4] Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Tomado de www.wikipedia.com
[5] Wireless fidely, mecanismo de conexión de dispositivos electrónicos de forma inalámbrica
[6] Computadoras Personales
[7] TELLEZ VALDEZ, Julio, "*Derecho Informático*", 3 Ed, Editorial Mc Graw Hill, México, 2014, pág. 103

criminalidad informática *va encaminado a la explotación de las redes de información y comunicación aprovechando las ventajas de la no existencia de barreras geográficas así como de la circulación de datos intangibles y volátiles*[8]

Ya se denota que el bien jurídico protegido es la información, donde la conducta antijurídica, culpable y punible se vale de medios informáticos cuyas funciones son el procesamiento y la transmisión automatizada de datos, la utilización de programas para cumplir su cometido.

Esta denominada criminalidad informática es cometida a través de las nuevas tecnologías y del internet, que hoy en día si bien es cierto es de mucha ayuda para las diversas actividades de una persona también se lo utiliza para el cometimiento de ilícitos evidenciándose una nueva forma de criminalidad en el medio.

La criminalidad informática esta generalmente dividida en dos grupos:

1. Crímenes que utilizan como instrumento o medio la tecnología.

2. Crímenes que tienen como finalidad u objetivo la tecnología como un ordenador, una red, un sistema operativo.

Los factores que conllevan el crecimiento de la criminalidad informática pueden ser de índole económica, social, política.

Los factores económicos, para aquellos quienes cometen dichos actos ilícitos tienen por objetivo el beneficio económico, por ejemplo el fraude informático.

En cuanto a lo social, al criminal informático le interesa obtener el poder, el pertenecer a una clase social privilegiada, el reconocimiento social, el

[8] GÓMEZ PEREZ, Mariana, "*Criminalidad informática, un fenómeno de fin de siglo*", ecured.cu,(Cuba): s.pág. Online. Internet. Consultado: 30 octubre 2015. Recuperado de: Recuperado de: http://www.ecured.cu/index.php/Criminalidad_inform%C3%A1tica

poseer más conocimientos que le ayuden a pertenecer a un status o un grupo elite.

La política, es un factor que les impulsa a realizar actos contrarios a la ley, a las personas o grupos quienes no están de acuerdo con políticas de gobierno, y en forma de protesta atentan contra los sistemas informáticos, por ejemplo el terrorismo. Con la única finalidad de desestabilizar el gobierno o de presionar a los mismos.

Sea la razón que conlleve a la criminalidad, se debe recalcar para que la conducta sea considerada como tal debe estar prevista en el ordenamiento jurídico de cada país, caso contrario así se tratase de una conducta que puede resultar delictiva pero si no está contemplada en la ley, no puede ser sancionada.

1.1.2 Delitos Informáticos

Una breve historia de la regulación de los delitos informáticos da el punto de partida en los Estados Unidos de Norteamérica, en donde en el año 1977 se presentó la primera propuesta de legislar por el senador Ribicoff en el congreso Federal.

Luego en el año 1983en Paris la OCDE[9] designa un grupo de expertos para que discutieran el crimen relacionado con las computadoras, esta organización luego del análisis recomendó a los países miembros la modificación de su legislación penal integrando los denominados delitos informáticos a fin luchar contra el problema del uso indebido de programas computacionales.

En el año 1989, el Consejo de Europa convocó a otro comité de expertos, quienes presentaron una pequeña lista de delitos informáticos que debían agregarse a las legislaciones penales de los países miembros con una lista opcional.

[9] Organización de Cooperación y Desarrollo Económico

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.

- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.[10]

En nuestro país tenemos como antecedente la Ley No. 2002-67 expedida el 10 de abril de 2002, que fue la LEY DE COMERCIO ELECTRÓNICO,

[10] "*Historia de los delitos informáticos*", delitosinformaticoslaschecks.blogspot.com. (Noviembre 2011): s.pág. Online. Internet. Consultado: 1 noviembre 2015. Recuperado de: http://delitosinformaticoslaschecks.blogspot.com/2011/11/historia-de-los-delitos-informaticos.html

FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, cuyo fundamento fue:

- La importancia que ha adquirido el uso de sistemas informáticos y redes electrónicas, inclusive el internet, en el ámbito público y privado.
- La necesidad de impulsar el acceso a las nuevas tecnologías a la población para el desarrollo del comercio, la educación y la cultura.
- La utilización de sistemas informáticos conllevaría a mejorar relaciones económicas y de comercio, actos, contratos civiles y mercantiles.

Actualmente esta ley fue derogada por la expedición del nuevo Código Orgánico Integral Penal que entro en vigencia el 10 de agosto de 2014, en donde los delitos informáticos han sido tipificados ampliamente.

Los Delitos informáticos, según Julio Téllez Valdez "son actitudes contrarias a los intereses de las personas en que se tiene a alas computadoras como instrumento o fin (concepto atípico) o a las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)"[11]

"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software"[12]

El delito según la legislación ecuatoriana *es la infracción penal sancionada con pena privativa de libertad mayor a treinta días.*[13] Y la infracción penal a su vez *es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código*[14].

[11] TELLEZ V., Julio, "Derecho Informático", 3 Ed, Editorial Mc Graw Hill, México, 2014, pág. 270.
[12] DAVARA Miguel Ángel, *"Derecho Informático*", Ed. Arzandi, España, 1993, págs. 318,319
[13] COIP, Art. 19, inciso primero.
[14] COIP, Art. 18.

Por delito informático se entenderá como aquella conducta típica, antijurídica y culpable mediante el uso indebido de cualquier medio tecnológico o informático.

De aquí se desprende el elemento objetivo y el elemento subjetivo del delito informático.

El elemento objetivo

En el delito informático este elemento varia pues dependerá si la tecnología es usada como medio o como finalidad, es así, que en algunos casos el delito tendrá como finalidad destruir o modificar los componentes de un ordenador, en otros casos el ordenador o la tecnología será utilizado como medio para la comisión del delito.

El elemento subjetivo

El elemento subjetivo se refiere a la culpa, es decir, que el sujeto del delito informático actué con conciencia y voluntad, por lo que debe comprobarse que lo hizo con dolo y culpa.

El dolo es el deseo de irrogar daño a otra persona o en sus bienes, con conciencia y voluntad produciéndose el resultado que está tipificado en la ley.

1.2 Conceptos y Definiciones

Al tratar el tema de los delitos informáticos imperiosamente se ve relacionado con terminología técnica, la misma que para su correspondiente comprensión en el desarrollo del trabajo investigativo, se procede a conceptualizar o definir siendo los siguientes:

Base de datos: serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.[15]

Cookie: es el nombre que recibe un lugar de almacenamiento temporal de información que usan páginas de internet.

Estas *cookies* son enviadas por páginas web y son almacenadas y administradas por los navegadores de internet. Son usadas comúnmente para guardar información relevante del usuario de una página.[16]

Firmware: "son microprogramas alojados en la memoria del computador o en un chip o circuito integrado que forma parte del hardeare; es un software en un hardware"[17]

Fraude: acto cumplido intencionalmente, con la finalidad de herir los derechos o intereses ajenos. Der civil. Derecho penal: el fraude es un elemento constitutivo del robo.[18]

Ftp o file transfer protocol (protocolo de transferencia de fichero) (sigla en inglés de file transfer protocol - protocolo de transferencia de archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red tcp (transmission control protocol), basado en la arquitectura cliente-servidor.

Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.[19]

[15] PERES VALDES, Damian, "*Que son las bases de datos*?", Maestros del Web,(octubre 2007): s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de: http://www.maestrosdelweb.com/que-son-las-bases-de-datos/
[16] CASTRO, Luis, "*Que es una cookie?",* About en español. s. pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://aprenderinternet.about.com/od/Glosario/g/Que-Es-Una-Cookie.htm
[17] NUÑEZ PONCE, Julio, "*Derecho Informático*", pág. 30, Lima –Perú, 1996
[18] CAPITANT, Henri, "*Vocabulario Jurídico*", Ediciones Depalma, Buenos Aires, 1961
[19] URBINA Gerardo," *QUE ES FTP?".*Blogspot. (abril 2010): s. pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://gerardo-urbinavelasco.blogspot.com/p/que-es-ftp.html

Hadware: es la parte física del ordenador constituida por los periféricos de entrada y salida. Se considera periféricos de entrada aquellos que permiten al usuario introducir datos, ordenes mediante comandos o programas al cerebro del ordenador, estos pueden ser el teclado, el mouse, cámara, scanner, micrófono, joystick, pantalla táctil, entre otros.

Mientras que los periféricos de salida son los que muestran al usuario los resultados de los datos u órdenes introducidos a la computadora, pudiendo ser la pantalla, los parlantes, la impresora, el plotter, data show, fax, etc.

Html (hyper text markup language): el lenguaje de computador usado para crear páginas de red para internet. Aunque estándares "oficiales" de internet existen, en la práctica son extensiones del lenguaje que compañías como netscape o microsoft usan en sus buscadores (browsers).

Http: http es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores.

El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.[20]

Internet: internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado tcp/ip.

Tuvo sus orígenes en 1969, cuando una agencia del departamento de defensa de los Estados Unidos comenzó a buscar alternativas ante una eventual guerra atómica que pudiera incomunicar a las personas. Tres años más tarde se realizó la primera demostración pública del sistema ideado, gracias a que tres universidades de california y una de utah

[20] URBINA Gerardo," *QUE ES HTTP?".*Blogspot. (abril 2010): s. pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://gerardo-urbinavelasco.blogspot.com/p/que-es-http.html

lograron establecer una conexión conocida como arpanet (advanced research projects agency network).[21]

Ip: toda computadora conectada a internet (o a cualquier red) posee una identificación única, llamada dirección ip (en inglés, internet protocol), compuesta por cuatro combinaciones de números (p.ej. 187.25.14.190). Estos números, llamados octetos, pueden formar más de cuatro billones de direcciones diferentes.

Cada uno de los cuatro octetos tiene una finalidad específica. Los dos primeros grupos se refieren generalmente al país y tipo de red (clases). Este número es un identificador único en el mundo: en conjunto con la hora y la fecha, puede ser utilizado, por ejemplo, por las autoridades, para saber el lugar de origen de una conexión.[22]

Lenguaje de programación: medios que permiten la comunicación entre el hombre y la máquina, es decir, entre la computadora y el usuario.[23]

Pharming: es la explotación de una vulnerabilidad en los equipos de los propios usuarios por bajos niveles de seguridad o antivirus, que permite a un atacante redirigir un sitio web diferente[24] al verdadero.

Protocolo de comunicación: conjunto de pautas que posibilitan que distintos elementos que forman parte de un sistema establezcan comunicaciones entre sí, intercambiando información.

Los protocolos de comunicación instituyen los parámetros que determinan cuál es la semántica y cuál es la sintaxis que deben emplearse en el proceso comunicativo en cuestión. Las reglas fijadas por el protocolo

[21] "*Definición de Internet*", definicion.de. s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://definicion.de/internet/#ixzz3Pttp471o
[22] "*Qué es la dirección IP*", InformaticaHoy. s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-la-direccion-IP.php
[23] TELLEZ VALDEZ, Julio, "*Derecho Informático*", 3 Ed, Editorial Mc Graw Hill, México, 2014, pág 12
[24] "*Pishing y otros*", Banco Pichincha. s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: https://www.pichincha.com/portal/Consejos-de-Seguridad/Phishing-y-otros

también permiten recuperar los eventuales datos que se pierdan en el intercambio.[25]

Sistema informático: conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.

Software: parte lógica del ordenador constituido por diversos tipos de programas usados en computación, lenguajes de programación y sistemas operativos.

URL: URL son las siglas de Localizador de Recurso Uniforme (en inglés Uniform Resource Locator), la dirección global de documentos y de otros recursos en la World Wide Web.

WWW: (World Wide Web) es un sistema de información y documentos vinculada a través de hipertexto e hipermedios a los que se puede acceder por medio de Internet, más específicamente, con un navegador web. [26]

[25] "*Definición de Internet*", definicion.de. s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://definicion.de/protocolo-de-comunicacion/
[26] "*Definición de WWW*", Definición ABC. s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de: http://www.definicionabc.com/tecnologia/www.php#ixzz3Ptzic9UB

CAPÍTULO II: EL DELITO INFORMATICO

2.1 Clasificación de Delitos Informáticos

Según el "*Convenio Sobre La Ciberdelincuencia*"[27] los clasifica de la siguiente forma:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

a) ***Acceso ilícito***: cuando se accede a un sistema informático infringiendo las medidas de seguridad con la finalidad de obtener datos u otra intención delictiva. Por ejemplo las aplicaciones móviles maliciosas para robar información de smarthphones.

b) ***Interceptación ilícita de datos:*** que por medios tecnológicos se intercepte de forma deliberada e ilegítimamente datos informáticos comunicados confidencialmente mediante un sistema informático.

c) ***Interferencia en los datos:*** comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

d) ***Interferencia en el sistema***: quien obstaculice grave, deliberada e ilegítimamente el buen funcionamiento de un sistema tecnológico o informático por medio de la introducción, transmisión, promoción de daños, borrado, deterioro, alteración o supresión de los datos informáticos.

e) ***Abuso de los dispositivos***: producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo o un programa informático que haya sido diseñado para la comisión de un delito informático. De igual manera si se trata de una contraseña, código de acceso o datos informáticos similares que permitan acceder a la totalidad o parte de un sistema informático con el fin de ser utilizados para cometer un delito.

[27] "*Convenio sobre la Ciberdelincuencia del Consejo de Europa*", AGDP.(noviembre 2001). s.pág. Online. Internet. Consultado: 25 enero 2015. Recuperado de https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Delitos informáticos

a) Falsificación informática: mediante la introducción, borrado o supresión de datos informáticos y que esto a su vez dé como resultado datos no auténticos con la intención de que los mismos sean utilizados como fidedignos para los efectos legales correspondientes.

b) Fraude informático: acto deliberado e ilegitimo que causa perjuicio patrimonial a una persona provocando un beneficio económico al cibercriminal o a una tercera persona, mediante la introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el normal funcionamiento de un sistema informático.

Delitos relacionados con el contenido

- ***Pornografía Infantil:*** Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

Son delitos en los cuales el delincuente reproduce y distribuye software que está legalmente prohibido su reproducción sin la autorización del autor.

También se los puede clasificar como instrumento o medio y por su finalidad u objetivo.

Instrumento o medio

Este tipo de conductas se ayudan de las computadoras, utilizadas como medio para el cometimiento del hecho ilícito.

a) ***Falsificación de documentos***: el delincuente se vale de medios tecnológicos para falsificar documentos por ejemplo tarjetas de crédito, cheques

b) ***Variación de los activos y pasivos:*** Al realizar los asientos contables de una empresa.

c) ***Simulation and Modeling:*** Planeación y simulación de delitos en donde se utiliza la computadora para planificar y controlar un delito.

d) ***"Robo" de tiempo de computadora***: cuando se utiliza laboratorios de programación produciendo grandes pérdidas en los sistemas de procesamiento de datos, si se efectúa cómputos con números de account ajenos. Por ejemplo en el caso de una empresa proveedora del servicio de internet que proporción una clave de acceso al usuario para la utilización del servicio pero este a su vez le facilita la clave a una tercera persona no autorizada para usarlo, produciendo perjuicio económico a la empresa proveedora.

e) ***Data Leakage*** Lectura, sustracción o copiado de información confidencial

f) ***Manipulaciones:*** Modificación de datos, que pueden afectar en la fase input que es la entrada de datos, output que es la salida de datos y en la fase de procesamiento de datos. Este tipo de manipulaciones puede producirse desde los ordenadores de la empresa o persona perjudicada o mediante un terminal que opere a distancia por ejemplo desde una computadora personal a través de una red telefónica.

g) ***Trojan Horse***: Conocido como Caballo de Troya, método más común para cometer un sabotaje, consiste en la introducción de instrucciones en la codificación de un programa o sistema para realizar funciones no autorizadas, inapropiadas o para que el programa actúe de forma diferente a la que está prevista siendo la persona quien lo ejecute el mismo usuario sin saberlo, por ejemplo formatear el disco duro.

h) ***Salami Techniques***: Técnica del salami consistente en la sustracción de pequeñas cantidades de activos o dinero de varias cuentas hacia una cuenta bancaria ficticia.

i) ***Superzapping:*** Uso no autorizado de programas de cómputo de acceso universal.

j) ***Trap Doors***: Puertas falsas, introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.

k) ***Logic Bombs:*** Bombas Lógicas, es la introducción de un programa que se ejecuta en un momento o fecha específica al cumplirse determinadas condiciones alterando el funcionamiento de los sistemas ya sea destruyendo o modificando la información o provocando que el sistema se cuelgue.

l) ***Scavening:*** Obtención o apropiación de información abandonada sin protección alguna producto residual de la realización de un trabajo que previamente estuvo autorizado, ya sea impresa en papel, en memoria o soportes magnéticos luego de la ejecución de un trabajo, también conocida como recogida de residuos.

m) ***Piggybanking and impersonation***: Parasitismo informático y suplantación de personalidad, es el acceso a áreas informatizadas en forma no autorizada obteniendo los sistemas o códigos privados de programas por engaños, que únicamente están bajo el manejo de personas en quienes se ha depositado un nivel de confianza importante ya sea por su capacidad o posición en la empresa. Se comete dos delitos a la vez la suplantación de identidad y el espionaje.

n) ***Wiretapping:*** Intervención en las líneas de comunicación de datos o teleproceso para acceder o manipular los mismos.

Fin u objetivo

La conducta criminal se dirige en contra del ordenador, programas o circuitos entendidos como entidad física.

a- *Programación de instrucciones que producen un bloqueo total al sistema*

b- *Destrucción de programas por cualquier método*

c- *Daño a la memoria*

d- *Atentado físico contra la maquina o sus accesorios (discos, cintas, terminales)*

e- *Sabotaje político o terrorismo en que se destruye o surja un apoderamiento de los centros neurálgicos computarizados.*

f- *Secuestro de soportes magnéticos en los que Figuera información valiosa con fines de chantaje, pargo de rescate.*

Finalmente se establece una clasificación mayoritariamente aceptada y que englobe las clasificaciones anteriores de una forma sintetizada, así:

La Organización de las Naciones Unidas, los clasifica así reconoce como delitos informáticos las siguientes conductas:

1. Fraudes cometidos mediante manipulación de computadoras:

a) Manipulación de los datos de entrada.

b) Manipulación de programas.

c) Manipulación de datos de salida.

d) Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas

a) Utilizando sistemas informáticos como objetos.

b) Utilizando sistemas informáticos como instrumentos.

3. Daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático.

b) Virus.

c) Gusanos.

d) Bomba lógica o cronológica.

e) Acceso no autorizado a sistemas o servicios.

f) Piratas informáticos o hackers.

g) Reproducción no autorizada de programas informáticos con protección legal.

2.2 Tipos de Delitos Informáticos

Una vez tratada las distintas clasificaciones de los delitos informáticos, corresponde sintetizar estas clasificaciones en los tipos de delitos informáticos, así lo establece el Dr. Santiago Acurio del Pino en su obra digital "Delitos Informáticos"[28]:

- Los fraudes
- El sabotaje informático
- El espionaje informático y el robo o hurto de software
- El robo de servicios
- El acceso no autorizado a servicios informáticos

2.2.1 El Fraude Informático

Utilización de un sistema informático de forma indebida con la finalidad de obtener beneficios económicos para sí mismo o para un tercero.

El fraude se produce al ingresar datos de manera ilegal, para lo cual el cyberdelincuente debe tener alto nivel de conocimientos informáticos, llevando a suponer que el mismo puede ser un empleado de una empresa que tiene acceso a sistemas o redes de información clasificada en donde puede ingresar y alterar datos para generar información falsa beneficiando al delincuente.

[28] ACURIO DEL PINO, Santiago, "*Delitos Informáticos* ", oas.org.págs. 22-29. Online. Internet. Consultado: 26 enero 2015. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Dentro del fraude informático tenemos:

Los datos falsos o engañosos

Conocida también como Data Diddling o manipulación de datos de entrada, que es la introducción o manipulación de datos falsos con la finalidad de producir movimientos falsos en transacciones de una empresa u organización.

Manipulación de programas o los "caballos de troya"

Conocido como ***Trojan* Horse**, consiste en la introducción de instrucciones, nuevos programas o nuevas rutinas de forma encubierta en el sistema de un ordenador con la finalidad de que realice una función determinada que no está autorizada o que es perjudicial para el sistema.

La técnica del salami

Técnica del salami o ***Salami Techniques*** consistente en la sustracción de pequeñas cantidades apenas perceptibles de dinero de varias cuentas hacia una cuenta bancaria ficticia, estas cantidades se van sacando repetitivamente de la cuenta del titular y se transfieren a otra mediante la introducción de instrucciones específicas al programa encargado de estas transacciones.

Falsificaciones informáticas

Como objeto:

Cuando el delincuente informático modifica datos de documentos que están almacenados en una base de datos computarizada.

Como instrumentos:

Cuando el delincuente informático se vale de medios tecnológicos para falsificar documentos de uso comercial por ejemplo tarjetas de crédito, cheques

Manipulación de los datos de salida

Modificación de datos, que afectan a la fase output que es la salida de datos, dicha manipulación es siempre con miras a un objetivo que es el funcionamiento del sistema informático. Por ejemplo el fraude a los cajeros automáticos con las tarjetas bancarias clonadas.

2.2.2 El Sabotaje Informático

El sabotaje informático es el acto por el cual se borra o modifica sin autorización el soporte lógico del ordenador, ya sean datos, programas o funciones, con la única finalidad de obstaculizar el normal funcionamiento del mismo.

Así lo indica la Dra. María Cristina Vallejo, el Sabotaje informático doctrinariamente, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.

Es acceder sin ser autorizados a servicios y sistemas informáticos que van desde la simple curiosidad, como es el caso de los piratas informáticos (hackers), hasta el sabotaje informático (cracking).

Este delito, puede entrañar una pérdida económica sustancial para los propietarios legítimos de Empresas, Instituciones públicas, privadas, Gubernamentales, etc..

El Sabotaje o Daño Informático puede tener lugar en Internet en dos formas: a).- Puede producirse por medio de la modificación y/o destrucción

de los datos o programas del sistema infectado, o b).- puede producirse por medio de la paralización o bloqueo del sistema, sin que necesariamente se produzca alteración ni destrucción de los datos o programas.[29]

Por lo tanto las técnicas comúnmente utilizadas son:

Bombas Lógicas

Logic Bombs, se produce mediante la introducción de un programa que se ejecuta en un momento o fecha específica posteriormente, al cumplirse determinadas condiciones alterando el funcionamiento de los sistemas ya sea destruyendo o modificando la información, o provocando que el sistema se cuelgue.

Una bomba lógica es difícil detectarla antes de que produzca el daño, por lo que se considera que poseen el máximo potencial de daño a diferencia de los virus o los gusanos que son fácilmente detectables y erradicables.

Gusanos

Los gusanos son parecidos a los virus pero con la diferencia que su finalidad es infiltrarse en programas para modificarlos o destruir los datos contenidos en el mismo pero una vez realizado su cometido no puede multiplicarse ni infectar otros archivos como los virus.

Virus informáticos y malware

Un virus informático es una amenaza programada, es decir, es un pequeño programa escrito intencionadamente para instalarse en el ordenador de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o al sector de "arranque" y se replica a sí mismo para continuar su propagación. Algunos se limitan solamente a replicarse, mientras que otros pueden producir

[29]VALLEJO, María Cristina, "*El sabotaje o daño informático*", Derecho ecuador, (Julio 2013): s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/el-sabotaje-o-dantildeo-informaacutetico

serios daños que pueden afectar a los sistemas. No obstante, absolutamente todos cumplen el mismo objetivo: PROPAGARSE[30]

El malware que al igual que los virus y los gusanos atacan las debilidades del ordenador desactivando controles informáticos y propagando los códigos maliciosos.

Ciberterrorismo

También denominado terrorismo virtual, mediante el cual el ciberdelincuente ataca masivamente el sistema de ordenadores de una entidad así como también puede atacar la estabilidad de un país mediante el ataque a sistemas gubernamentales. El ejemplo más claro es Anonymous, y sus acciones se basan en ataques DDoS, desconfiguración de webs o publicación de datos comprometidos.

Se considera ciberterrorismo de igual manera a la difusión de noticias falsas en la red.

Ataques de denegación de servicio

Consiste en la utilización de recursos del sistema informático con el objetivo de que se congestione y que ningún usuario mas pueda usarlo perjudicando al servicio pleno que debe ofrecer el sistema atacado.

2.2.3 Espionaje Informático

El espionaje informático según Marcelo Huerta Miranda, es toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información.[31]

[30] "*Concepto de virus informático",* nisu.org. s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de http://spi1.nisu.org/recop/al01/salva/definic.html

[31] HUERTA MIRANDA, Marcelo, "*Figuras delictivo-informaticos tipificadas en Chile*" Alfa-redi. (marzo 2002): s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de: http://www.alfa-redi-org/rdiarticulo.shtml?=433

Fuga de datos (data leakage),

Consiste en la lectura, sustracción o copiado de información confidencial o datos reservados. Por ejemplo el Ciberespionaje industrial que consiste en el robo de información a empresas.

Reproducción no autorizada de programas informáticos de

Protección legal.

En este tipo de delito se ve directamente afectado los derechos de autor y la propiedad intelectual, pues consiste en realizar copias de programas informáticos protegidos legalmente y cuya reproducción no esta autorizada.

2.2.4 Acceso no autorizado a servicios informáticos

El acceso no autorizado a servicios informáticos según Claudio Libano Manzur es un delito informático que consiste en acceder de manera indebida, sin la autorización o contra derecho a un sistema de tratamiento de información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o contraseñas, no causando daños inmediatos y tangibles en la victima, o bien por la mera voluntad de curiosear o divertirse de su autor.[32]

Las puertas falsas (trap doors),

Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios.

La llave maestra (superzapping)

Uso no autorizado de programas de cómputo de acceso universal mediante un programa que abre cualquier archivo así este esté protegido con la finalidad de alterar, borrar, copiar, modificar o utilizarlo en cualquier forma no permitida los datos contenidos en el ordenador.

[32] Ibídem.

Pinchado de líneas (wiretapping)

Intervención en las líneas de comunicación de datos o teleproceso para acceder o manipular los mismos. Para evitar este tipo de delito se debe transmitir la información criptografiada, esto es mediante el método de la criptografía que es la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para:

- Autentificar la identidad de usuarios;

- Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias;

- Proteger la integridad de transferencias electrónicas de fondos.[33]

Piratas informáticos o hackers.

El pirata informático o hacker, es una persona experta en el manejo de los sistemas informáticos quienes acceden a los mismos de manera no autorizada ya sea aprovechándose de las deficiencias en las medidas de seguridad o del descuido de los usuarios en cuanto a las contraseñas.

2.3 Características de los Delitos Informáticos

El autor Julio Téllez Valdez establece las principales características de las acciones que configuran el delito informático:

a) *Conductas Criminógenas de cuello blanco*: se refiere a que únicamente personas con conocimientos técnicos en el área de la informática pueden cometerlos.

b) *Son acciones ocupacionales:* cuando el sujeto se encuentra trabajando.

[33] "*Criptografia. Seguridad Informática".* Informatica Hoy. s. pág. Online. Internet. Consultado: 15 enero 2015. Recuperado de: http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Criptografia-Seguridad-informatica.php

c) *Son acciones de oportunidad:* el sujeto lo realiza aprovechando una ocasión creada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) *Provocan serias pérdidas económicas:* quienes realizan será principalmente con una intención de beneficiarse económicamente, produciendo un decremento patrimonial al sujeto pasivo.

e) *Ofrecen facilidades de tiempo y espacio:* susceptibles a ser realizados en tan solo segundos y sin necesidad que el sujeto se encuentre físicamente puede consumarse el hecho.

f) *Son muchos los casos y pocas las denuncias:* muchas de las veces por vacíos jurídicos, o por la dificultad probatoria.

g) *Son muy sofisticados y relativamente frecuentes en el ámbito militar;* en este ámbito suele suceder por cuanto el personal está altamente capacitado para trabajar con equipos de última tecnología que le facilita el cometimiento del ilícito.

h) *Presentan grandes dificultades para su comprobación:* el sujeto no suele dejar evidencias.

i)Son imprudenciales: se los cometen por descuido, con respecto a esto se debe discrepar porque el sujeto no actúa imprudentemente, sino al contrario con voluntad y conocimiento del hecho.

j)Ofrecen facilidades para su comisión a los menores de edad: se ven en la red tutoriales de cómo pueden hackear cuentas de un app store por ejemplo, y está al alcance de todos inclusive los niños y adolescentes.

k) *Tienden a proliferar cada vez más:* la tecnología avanza y nuevas formas de atacar a esta tecnología y hacer mal uso de la misma aparecen, por lo que se hace necesario una regulación.

l)*Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley:*[34] las legislaciones tratan de regular el mayor tipo de hechos delictivos de esta índole, sin embargo, no es suficiente puesto que siempre habrán nuevos ataques no previstos en la ley.

[34] TELLEZ V., Julio, "*Derecho Informático*", 3 Ed, Editorial Mc Graw Hill, México, 2014, pág. 270.

2. 4 Elementos del Delito Informático

2.4.1 Sujeto activo

El sujeto activo es quien comete el hecho delictivo o cuya conducta se adecua al tipo penal.

Los delitos informáticos son conocidos criminológicamente como “delitos de cuello blanco”, denominación dada por el sociólogo estadounidense Edwin H. Sutherland quien acuño la expresión "cuello blanco" en un discurso ante la Asociación Americana de Sociología el 27 de diciembre de 1939 En su monografía de 1949, los delitos de cuello blanco se definen como "un crimen cometido por una persona de respetabilidad y de alto estatus social en el curso de su ocupación".

La razón es por cuanto el sujeto activo no puede ser cualquier persona sino que debe tener una preparación técnica, habilidades para manejar sistemas informáticos, conocimientos de lugares estratégicos los cuales son vulnerados, ser técnicos o profesionales en sistemas informáticos lo que le diferencia de un delincuente común.

Al sujeto activo de estos delitos se lo conoce como delincuente informático o cibercriminal, pero tiene distintas denominaciones, siendo las más conocidas las siguientes:

Hacker: es una persona que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo.[35]

El hacker es una persona experta en el manejo de sistemas de ordenadores, quien accede a los mismos sin autorización, en forma indebida, con la finalidad de robar información, producir daños en el

[35] CASTRO, Luis, *¿Qué es "hacker"?,* about en español. s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de: http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm

sistema, o simplemente por una satisfacción intelectual como la curiosidad de descifrar el password de acceso sin causar daños a la victima, principalmente se burla de los sistemas de seguridad.

Craker: Un hacker es un individuo que crea y modifica software y hardware de computadoras, para desarrollar nuevas funciones o adaptar las antiguas, sin que estas modificaciones sean dañinas para el usuario del mismo.

Los hackers y crackers son individuos de la sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, pero la diferencia básica entre ellos es que los hackers solamente construyen cosas para el bien y los crackers destruyen, y cuando crean algo es únicamente para fines personales.[36]

Para llegar a ser craker debe ser primero un hacker quien conoce perfectamente el manejo de un software y posteriormente se perfecciona con el manejo del hardware o la parte física de un ordenador, por tanto un craker conoce la programación y la parte física de la tecnología.

Se caracterizan por aquella capacidad para romper sistemas exclusivamente, es decir, romper protecciones que tiene un software y además lo difunde en la red para compartir dicho conocimiento a los demás ya sea gratuitamente o en el mercado negro obteniendo beneficios económicos.

Al craquear un programa o romper sus seguridades, crean copias masivas y le asignan códigos por ejemplo los cds con software pirata de Windows 8 instalándolo en ordenadores cuyos usuarios pueden tener conocimiento o no, de la licitud de su origen, quienes no lo saben llegan a creer que tienen las versiones originales puesto que el programa crakeado inclusive presenta certificados de garantía de procedencia.

[36] *¿Qué es craker?,* Informática Hoy. s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

Los cracker se dedican a desproteger los programas de todo tipo por ejemplo los que se comercializan bajo con la etiqueta “anti-copia”, como los que se instalan bajo la denominación “a prueba” para que estos resulten operativos indefinidamente.

Utilizan la ingeniería inversa que consiste en desarmar un programa hasta llegar a la protección de seguridad que generalmente se encuentran en el sistema operativo, y producir la rotura ahí, que representa el ya no tener que pagar por un programa a prueba y que caduque en un número de días por ejemplo.

Phreacker: Un phreaker es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.[37]

Denominado también cracker de teléfono o fonopirata, quien posee conocimientos de informática, de redes telefónicas y redes móviles, buscan burlar la protección de las redes públicas y corporativas de telefónica, cuya finalidad varia, puede ir desde utilizar el servicio sin pagarlo hasta la reproducción fraudulentas de tarjetas prepago para llamadas telefónicas

Virucker: Un virucker se dedica básicamente a la programación de virus informáticos. Cuya finalidad varían, pudiendo ser:

- Ser admirado aunque anónimamente por ser el autor de dicho virus.
- Experimentar creando nuevos virus.
- Producir daño al sujeto pasivo ya sea una persona natural o una persona jurídica.
- Motivaciones políticas o terroristas
- Difundir ideas radicales a manera de protesta.

[37] “*Definición de Phreaker*”, Infoseguridad. (Marzo 2008): s.pág. Online. Internet. Consultado: 2 febrero 2015. Recuperado de http://inforleon.blogspot.com/2008/03/definicion-de-phreaker.html

Pirata informático: es aquel individuo que reproduce y distribuye a título gratuito u oneroso un software sin permisos legales del autor.

El pirata informático suele tener bajo su dominio sitios web en donde ofrece software gratuito infringiendo los derechos de autor a cambio de que los usuarios suban o carguen a la página otros programas.

Perfil criminológico del delincuente informático y su anonimato

Según el Dr. Cesar Ramírez Luna los delincuentes informáticos, son personas especiales (utilizan su inteligencia superior a la normal, para adquirir los conocimientos en esta materia para poder desarrollar comportamientos ilegales). Generalmente son personas poco sociables, que actúan preferentemente en la noche; son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita. Los Hackers posmodernos corsarios de la red, constituyen la última avanzada de la delincuencia informática de este final de siglo.[38]

Razón por la cual se los llego a denominar delitos de cuello blanco, pues solo ciertas personas pueden ser catalogados como delincuentes informáticos quienes reúnen características peculiares como lo menciona el Dr. Ramírez.

Por otro lado el sujeto activo de los delitos informáticos generalmente es anónimo esto para evadir su responsabilidad, siendo conocidos únicamente por seudónimos, el anonimato va más allá de la no utilización de sus datos personales sino que también para el cometimiento del ilícito pueden recurrir a la utilización de sistemas informáticos de un tercero o utilizando programas de enmascaramiento que oculten su ubicación y a cambio muestren una ubicación falsa mediante un IP falso.

[38] RAMIREZ LUNA, César, "*EL PERFIL CRIMINOLOGICO DEL DELINCUENTE INFORMATICO* ",derecho.usmp. s.pág. Online. Internet. Consultado: 3 febrero 2015. Recuperado de: http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

2.4.2 Sujeto pasivo

El sujeto del delito pasivo es sobre quien recae la conducta delictiva es decir, la víctima del delito, en el caso de los delitos informáticos es sobre las bases de datos de las personas que pueden ser personas naturales o personas jurídicas y estas últimas de derecho público o derecho privado.

En la actualidad se ha visto una evolución, por cuanto antes no se denunciaban los delitos informáticos porque no había forma de establecer el modus operandi del sujeto activo, al ser un delito computacional, el delincuente lo realizaba en cuestión de minutos y podía borrar las evidencias, haciendo imposible determinar la responsabilidad y la identidad del ciberdelincuente.

2.4.3 Bien jurídico protegido

El bien jurídico protegido, en los delitos informáticos, de los ataques o de la conducta del sujeto activo es la INFORMACION que es susceptible a ser almacenada, tratada y transmitida a través de sistemas informáticos, reconociendo que dicha información tiene un valor económico para el titular de la misma.

Por ello el patrimonio de muchas empresas se trata de un tipo de acervo informático que le sirve para la gestión administrativa de la misma o para tomar decisiones y en el caso de caer esta información en manos criminales puede ser utilizada en beneficio propio y puede ser dañada, destruida o alterada provocando pérdidas económicas para la empresa.

Tratando en el ámbito particular, la información de una persona que represente valor económico, si cae en manos de terceras personas de manera irregular y hacen mal uso de la información obtenida como consecuencia se tendrá el decremento del patrimonio del sujeto pasivo, es decir, a quien le pertenece la información sustraída.

De igual manera hay la información puede ser de índole personal, así lo establece la Dra. **Regina Zambrano Reyna**[39] en su publicación "Delitos contemplados en la ley ecuatoriana", al cometimiento de un delito informático se viola lo que es más privativo de un ser humano como son los bienes intangibles amparados por el Derecho de Propiedad al manipularse sus datos personales y privados considerando que desde un nombre de dominio, una creación intelectual de cualquier índole, intimidad personal, dirección virtual o convencional, cometimiento de fraude, conlleva la seguridad jurídica en la red[40]

Los delitos informáticos pueden perjudicar al honor, al buen nombre, derechos a los que esta asistido la persona, como por ejemplo el caso de robo o usurpación de identidad, que haciéndose pasar por otra persona el sujeto activo cometa hechos delictivos y esto afecta directamente al sujeto pasivo.

Por lo que la Información, como bien jurídico tutelado, también engloba:

La reserva, la intimidad y confidencialidad de los datos: cuando lo que se busca es agredir la esfera de la intimidad en forma general de una persona mediante el mal uso de los medios informáticos como por ejemplo el robo de identidad.

La seguridad o fiabilidad del tráfico jurídico y probatorio; utilizado principalmente en un proceso judicial en donde se torna necesario el uso de datos o documentos a través de medios informáticos como pruebas, en estos casos puede darse las falsificaciones.

El derecho de propiedad: cuando con el delito informático se pretende atacar a la información o a los elementos físicos, materiales de un sistema informático, claro ejemplo el terrorismo informático.

[39] Doctora en Jurisprudencia, especialista en Derecho Informático, Propiedad Intelectual, Derecho Ambiental.
[40] ZAMBRANO REYNA, Regina, "*Delitos Informáticos*", *cecs.espol.* s.pág. Online. Internet. Consultado: 4 febrero 2015. Recuperado de: http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf

CAPÍTULO III: EL FRAUDE INFORMÁTICO

Originariamente el fraude dentro del área penal, fue vinculado con el delito de la estafa, a tal punto que muchas veces al tratar de fraude y estafa se los consideraba como sinónimos, sin embargo, con los adelantos tecnológicos se hizo imprescindible el instituir una figura penal relacionada con la época tecnológica y que se adecue a la misma, debido a que los delincuentes se aprovechaban de la informática para cometer el ilícito.

Por lo que el delito de la estafa era un tipo incapaz de contener un sin número de nuevas acciones, cuya novedad o característica esencial era la defraudación con la ayuda de medios tecnológicos, naciendo el Fraude Informático como un nuevo tipo delictivo.

Este nuevo tipo penal dentro del Derecho Penal y a su vez en el Derecho Informático abarcaba el mayor tipo de conductas defraudatorias que tenía incorporada a la informática como medio de la comisión.

El Fraude Informático es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.[41]

Es un tipo de delito informático perpetrado mediante medios tecnológicos, es decir, por la utilización de un sistema informático con la finalidad de transferir activos patrimoniales a favor del cibercriminal o de terceros. Se trata de un delito netamente virtual, esto quiere decir, que no sería posible efectuarlo de manera física como por ejemplo un hurto, sino que es necesario para su perfeccionamiento la utilización de las redes y de un sistema informático.

En la actualidad la globalización y los adelantos tecnológicos, han beneficiado a la sociedad en general pero también a la par han propiciado la delincuencia virtual, en este sentido, el Fraude Informático, en donde el ánimo del delincuente es el obtener beneficios económicos provocando grandes pérdidas económicas, y cada vez es mayor este delito en el medio, provocando su regulación ampliamente, las posibilidades son variadas y cada vez se crea una nueva modalidad de la comisión del Fraude Informático.

3.1 Modalidades de Fraude Informático

Las modalidades de Fraude Informático más comunes son:

3.1.1 Manipulación de los datos de entrada o sustracción de datos

Este tipo de Fraude Informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.[42]

El sujeto activo del fraude en esta modalidad generalmente conoce el propósito del programa manipulado o de los datos introducidos ya por ser empleado o tener como cómplice a un empleado de la compañía, por lo que su trabajo lo hará minuciosamente para que dicho fraude no pueda ser descubierto luego, convirtiéndose difícilmente detectable.

La acción en sí, consiste en tomar datos introducidos previamente en el ordenador, es decir, procesados, sustrayéndolos a través de medios de almacenamiento con la finalidad de ser leídos y manipulados

[42] ESTRADA CABRERA Yamilka, RAMOS ÁLVAREZ Everardo Luis, *"El fraude informático. Consideraciones generales"*, Contribuciones a las Ciencias Sociales, (Noviembre 2011): s.pág. Online. Internet. Consultado: 5 febrero 2015. Recuperado de: http://www.eumed.net/rev/cccss/14/ecra.html

posteriormente en otros ordenadores, o simplemente sustraer dichos datos para uso exclusivo del cyberdelincuente o de un tercero con un fin específico.

Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede acceder a todo tipo de registros y programas.

3.1.2 La Manipulación de programas

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Como ejemplo está el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.[43]

Mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.

3.1.3 Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados

[43] HALL, Andrés, "*Tipos de delitos informáticos: Los tipos de delitos informáticos reconocidos por Naciones Unidas"*, forodeseguridad.com, s.pág. Online. Internet. Consultado: 5 febrero 2015 Recuperado de: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.[44]

Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo.

3.1.4 Fraude efectuado por manipulación informática

Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.[45]

Accediendo a los programas establecidos en un sistema de información, y manipulados para obtener una ganancia monetaria.

Además de los anteriores, se puede anotar dos modalidades muy conocidas en el medio actual como son el phishing y el pharming.

3.1. 5 Phishing

El "phishing" es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.[46]

Opera generalmente suplantando la imagen de una empresa o entidad pública haciendo creer al usuario que los datos solicitados provienen del sitio web oficial siendo en realidad un sitio falso, que se aprovecha de dichos datos para luego ser ingresados en la página oficial y realizar actos

[44] Ibídem

[45] ESTRADA CABRERA Yamilka, RAMOS ÁLVAREZ Everardo Luis, *"El fraude informático. Consideraciones generales"*, Contribuciones a las Ciencias Sociales, (Noviembre 2011): s.pág. Online. Internet. Consultado: 5 febrero 2015. Recuperado de: http://www.eumed.net/rev/cccss/14/ecra.html

[46] LUQUE GUERRERO, José María, *"Qué es el phishing y cómo protegerse",* internautas.org, (Mayo 2005): s.pág. Online. Internet. Consultado: 8 febrero 2015. Recuperado de http://seguridad.internautas.org/html/451.html

fraudulentos en perjuicio del titular que sin la debida seguridad proporciono a la página falsa.

Mediante este método el cyberdelincuente puede obtener datos como:

- Los números de su tarjeta de crédito o débito.
- Números de cédula o pasaportes.
- Claves secretas.
- Contraseñas.
- Coordenadas e-key.
- Direcciones.
- Teléfonos.

Dicha información le servirá para realizar transacciones electrónicas fraudulentas perpetrándose así el delito.

Los ciberdelincuentes que utilizan esta modalidad de fraude, crean paginas falsas migrando de un país a otro por lo que son difíciles de ser rastreados, ofertando la información en el mercado de cada país al que robaron, es más, para mantenerse en el anonimato y no ser rastreados llegan a utilizar la Deep web para ofrecer la información hackeada.

Las formas de phishing pueden ser varias, pero las más usuales son:

- *Mensajes Cortos (SMS):* Envió de mensajes a usuarios solicitando datos personales. En nuestro medio se ejemplifica con la oleada de mensajes aseverando que el usuario ha ganado un sorteo y para reclamar el mismo debe proporcionar información confidencial.
- *Llamadas Telefónicas*: El usuario recibe una llamada telefónica en donde el emisor suplanta la identidad de un funcionario o empleado de entidad privada o pública solicitando datos privados.
- *Páginas Web*: Simulación de la página web oficial de la entidad requerida, por ejemplo una página web falsa del banco del pichincha. También se realiza mediante sitios web falsos con señuelos llamativos, como por

ejemplo aquellas que aparecen como ventanas emergentes con la consigna “Eres el usuario #1 millón, te has hecho acreedor de un Iphone, da click aquí”, en donde le piden al usuario que facilite datos personales con la única finalidad de ser mal utilizados. De igual en el correo electrónico por medio de los spam[47].

Los principales daños provocados por el phishing son:

- Robo de identidad y datos confidenciales de los usuarios, esto puede conllevar pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas.

- Pérdida de productividad.

- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.).[48]

3.1.6 Pharming

El término "pharming" es una combinación de las palabras "phishing" (suplantación de identidad) y "farming" (agricultura), que se usa así, porque una forma de este cibercrimenes esencialmente una estafa mediante phishing que puede afectar a varios usuarios a la vez.[49]

Se trata de una variante del phishing, pues si bien la finalidad es de llevar al usuario a la página falsa y solicitarle información personal, la diferencia radica en que el pharming utiliza técnicas diferentes para conseguir dicha información, engañando no al usuario sino al ordenador para que cambie los números IP de una dirección URL correcta, llevando al usuario a otro destino distinto al original.

[47] Correo electrónico no deseado.
[48] “*Phishing”,* pandasecurity.com,. s.pág. Online. Internet. Consultado: 10 febrero 2015. Recuperado: dehttp://www.pandasecurity.com/ecuador/homeusers/security-info/cybercrime/phishing/
[49] *“¿Qué es pharming?”,* Kapersky.com, .pág. Online. Internet. Consultado: 11 febrero 2015. Recuperado: http://latam.kaspersky.com/mx/internet-security-center/definitions/pharming

En este caso el usuario difícilmente puede cerciorarse de que está en peligro pues ingresa a una dirección correcta pero le lleva a un servidor diferente.

Al vulnerar un servidor DNS o un router todos los usuarios de ese servicio pueden ser víctimas, esto le diferencia del phishing que se centra en una sola persona.

3.2 Casos de Fraude Informático

Equity Funding Corporation de América

Uno de los primeros casos conocidos del mal uso de la tecnología de la información ocurrió en Equity Funding Corporation de América, desde el año 1964 hasta 1973, los gerentes de la compañía reservaron pólizas de seguros falsas para mostrar mayores ganancias, incrementando así el precio de la reserva de la compañía. Luego de que el fraude se descubrió, le tomó a la firma de revisión Touche Ross dos años para confirmar que las pólizas de seguros eran ficticias.

Este fraude se descubrió exactamente en el año 1973, en donde las cifras aproximadas fueron de dos billones de dólares, sus inicios fue en el año 1964 cuando la Gerencia de la compañía empezó a defraudar durante casi diez años, el fraude en si consistía de 3 etapas:

Fase de inflar ingresos: inflar ingresos por medio de comisiones, simuladas que fueron obtenidas por los préstamos hacia los clientes.

Fase extranjera: la empresa adquirió otras empresas que fueron subsidiarias en el extranjero, con la finalidad de realizar transferencias a las mismas de bienes, simulando que los clientes que supuestamente habían adquirido préstamos los estaban pagando.

Fase de Seguros: la empresa revendía las pólizas de seguros a otras aseguradoras, siendo una práctica normal dentro del ámbito en el caso de que una compañía necesite urgentemente fondos solucionando el

problema de liquides a corto plazo, en este caso la Equity Funding creó pólizas falsas para venderlas a otra compañía.

El fraude informático se lo comete en esta última fase, debido a que las pólizas ficticias solo podían haber sido creadas mediante la utilización de un medio informatizado.

La compañía quebró generando un desastre financiero ascendiendo el perjuicio económico a 2 millones de dólares, de lo cual el 10% fue producto del Fraude de seguros.

El caso Security Pacific National Bank

Este caso sucedió en 1978 en los Ángeles de California, en donde Stanley Mark Rifkin un analista informático quien con sus conocimientos y haciendo uso de técnicas de ingeniería social consiguió efectuar un robo colosal al Pacific National Bank mediante la manipulación de la red de manejo interno de datos informáticos (TEF) del sistema de reserva federal[50] y se apropió de diez millones doscientos mil dólares.

Rifkin realizaba trabajos de consultoría en el Security Pacific National Bank por lo que tenía acceso a los sistemas informáticos del mismo, el 25 de octubre de 1978 visita dicha entidad en donde al considerarle parte del personal de seguridad informática del banco le dieron paso a las instalaciones llegando al nivel D en donde se encontraba la sala de transferencias lugar en el que se encontraba anotado en la pared el código secreto de transferencias, este código cambiaba diariamente y es el que permitía autorizar las transferencia, memorizo el código y salió del lugar.

Enseguida, los empleados de la sala de transferencia recibieron órdenes de otro empleado encargado de la división internacional del banco, mediante una llamada telefónica ordeno una transferencia sistemática de fondos a una cuenta en el Banco de New York, Irving Trust Company

[50] Agencia gubernamental que permite a los bancos transferir fondos de un banco a otro en los Estados Unidos y en el extranjero

proporcionando el código secreto del día para autorizar la transferencia por un monto de 10.2 millones de dólares. Esta persona no era sino el mismo Stanley Rifkin, pero los empleados del banco nunca se percataron hasta el mes de noviembre donde el FBI mediante investigaciones detectaron el fraude.

Pero para Rifkin la transferencia no era suficiente, sino que debía utilizarlo en algo que fuese imposible de rastrearlo, por lo que en octubre empezó a convertir los fondos robados en diamantes, ofreciendo pagar a la empresa Russalmaz 8,145 millones de dólares a cambio de 43.200 quilates de diamantes, haciéndose pasar por el representante de Coast Diamond Distributors.

Posterior a ello, Rifkin introdujo de contrabando los diamantes a Estados Unidos y empezó a comercializarlos a distintos joyeros, pero uno de ellos que tenía conocimiento del fraude al Pacific National Bank se contactó con el FBI quienes le dieron el seguimiento al caso para finalmente allanaron el domicilio de Rifkin encontrando la evidencia como diamantes y dinero en efectivo. Luego de ello al salir bajo fianza intento usar nuevamente el mismo sistema con el Union Bank de los Angeles pero no le fue posible, siendo arrestado, juzgado y sancionado con ocho años de prisión.[51]

El caso de Fraude Informático más grande en Estados Unidos

Considerado el mayor caso de fraude más grande de la historia en donde han sido acusados 5 personas, cuatro de ellos rusos Vladimir Drinkman, Aleksander Kalinin, Roman Kotov y Smilianets Dmitriy y uno ucraniano Mikhail Rytikov, fueron acusados por el Departamento de Justicia de los Estados Unidos porque presuntamente robaron unas 160 millones de tarjetas de crédito y débito de grandes corporaciones como NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea,

[51] Fuente: http://www.securityartwork.es/2009/12/21/seguridad-e-historia-el-caso-del-security-pacific-national-bank/

Dexia, JetBlue, Dow Jones, Euronet, Visa Jordania, Pago Global, Diners Singapur y Ingenicard durante aproximadamente 7 años.

El dinero defraudado no se ha logrado calcular con precisión pero se estima en cientos de millones de dólares, sin embargo se sabe que 300 millones de dólares fueron robados de las empresas Nasdaq, Visa y Dow Jones.

Su modus operandi consistía en primer lugar instalar un malware en las bases de datos de las grandes corporaciones que se introducían a los archivos y robaban datos de las tarjetas de crédito y de débito para luego venderlas al mejor postor, cobrando aproximadamente $10 para cada número de tarjeta de crédito estadounidense, $50 para la tarjeta de crédito europea y $15 para la tarjeta canadiense.

Las penas si es que se demuestra su responsabilidad, serán conforme a la cuantía del dinero que presuntamente fue robado, si se demuestra el Fraude Informático podrían enfrentar hasta 30 años de prisión y una multa de un millón de dólares el doble de la ganancia o pérdida del delito. [52]

3.3 Legislación Ecuatoriana

El fraude informático en el Ecuador ha ido creciendo desmesuradamente, tan solo una referencia la tenemos en la publicación en la página web del diario El Telégrafo con fecha 17 de septiembre de 2012 que indica:

"*En julio de 2011 la presidenta del Consejo de Participación Ciudadana y Control Social (Cpccs), Marcela Miranda, denunció el desvío de 20 mil dólares de las cuentas bancarias de 47 funcionarios de esa entidad.*

[52] Fuente: Neowin.net

Según la denuncia presentada ante la Fiscalía de Pichincha, el dinero desapareció de las cuentas de los empleados a través de transferencias realizadas al exterior.

José Vásquez, abogado patrocinador de los afectados, señaló en días posteriores al hecho que las cuentas de los funcionarios estaban de diez bancos distintos, entre ellos, Guayaquil, Pacífico, Pichincha, Amazonas, Machala y Produbanco, cuyos montos retirados fueron entre los 2 y 50 mil dólares.

Esos son algunos de los casos de delitos informáticos que han trascendido en el país, donde uno de los sectores más afectados es el financiero, perjudicando no solo el patrimonial del Estado sino también el de centenares de clientes desde 2009, cuando se empezó a hablar de esa modalidad delictiva.

Desde entonces, las autoridades han registrado un incremento de denuncias hasta situarse en 4.287 casos. Esa cifra contempla los robos denunciados hasta junio del presente año, pero existiría un subregistro de aquellas personas que no reportaron la pérdida.

El director de Tecnologías de la Información de la Fiscalía, Jorge Luis San Lucas, informó que entre los delitos identificados está el conocido 'pishing', que consiste en la creación de páginas web falsas de bancos para obtener datos de los clientes y así ingresar a las cuentas reales y robar dinero.

Dijo que se está dando con fuerza el ataque a los cajeros automáticos, por medio del 'skiming', el cual consiste en la colocación de dispositivos externos al cajero que sirven para copiar las claves de las tarjetas y clonar las bandas magnéticas.

Además, constan en ese listado, la revelación ilegal de base de datos, los daños informáticos, la obtención de información no autorizada, modificación e inutilización de programas, los delitos contra la información pública

empleando diversos medios informáticos para su ilegal obtención, manipulación o distribución para fines ilícitos.

Se observa que en el país los delitos informáticos cada vez son más, siendo urgente regularlos y sancionarlos conforme a la realidad actual.

Como antecedente dentro de la legislación Nacional fue la expedición de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas siendo aprobada definitivamente en abril del año 2002, el auge del comercio electrónico fue la razón fundamental para la creación de esta ley, para dar seguridad jurídica a las relaciones que tenían vinculación íntima con la tecnología y a la vez ante el asecho de la criminalidad informática que siempre va a la par con los adelantos tecnológicos.

Pero la tecnología se desarrolla rápidamente y cada día se muestra adelantos en el área técnica informatizada, dando lugar a que el delito informático también evolucione, tornándose indispensable una nueva propuesta dentro del marco jurídico legal, en donde se trate de comprender el mayor tipo de delitos informáticos, disminuyendo así la inseguridad jurídica que envuelve hoy en día a la sociedad de la tecnología.

Código Orgánico Integral Penal

Actualmente en el Ecuador se encuentra vigente el Código Orgánico Integral Penal que derogó al antiguo Código Penal y otras leyes entre ellas la anterior Ley de Comercio Electrónico, Mensajes de Datos y Firmas. El COIP está vigente desde agosto del año 2014.

En este nuevo cuerpo legal los Delitos Informáticos se encuentran normados en el Código Orgánico Integral Penal, en el Libro Primero *La Infracción Penal*, en los siguientes artículos:

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

–Artículo 229.- Revelación ilegal de base de datos
–Artículo 230.- Interceptación ilegal de datos
–Artículo 231.- Transferencia electrónica de activo patrimonial
–Artículo 232.- Ataque a la integridad de sistemas informáticos
–Artículo 233.- Delitos contra la información pública reservada legalmente.
–Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

Lo que se refiere específicamente al Fraude Informático se encuentra regulado en el Capítulo Segundo Delitos Contra Los Derechos De Libertad, Sección Novena Delitos Contra El Derecho A La Propiedad, en el art. 190.

Artículo 190.- *Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.*

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Análisis del Tipo Penal:

- *Sujeto activo:* Cualquier persona
- *Sujeto pasivo*: (El ofendido) Cualquier persona.
- *Bien jurídico protegido*: La propiedad, la información.

- *Verbo rector*: apropiar, transferir, facilitar, manipular, modificar.
- *Condicionantes*: se utilice medios electrónicos: sistemas informáticos, *redes electrónicas* o de telecomunicaciones.
- *Pena a imponerse***:** Prisión de uno a tres años**.**

En el art. 190 se regula la apropiación fraudulenta, es decir, con fines económicos, siempre que la persona utilice un sistema informático como lo es el ordenador o computadora.

También menciona las redes electrónicos o de telecomunicaciones, pudiendo ser estas aquellas que sirven para interconectar dispositivos, comunicarse y compartir recursos, archivos, etc.

Teniendo como fin u objetivo la apropiación o transferencia no consentida de bienes, valores o derechos almacenados en bases de datos susceptibles a ser manejados virtualmente, generando un perjuicio para el titular de los mismos y un beneficio para el cyberdelincuente o una tercera persona.

El artículo regula el Fraude Informático y dentro de este las modalidades: manipulación en la entrada de datos, manipulaciones en el programa al referirse a la manipulación y modificación de funcionamiento de sistemas informáticos, descubrimiento o descifrado de claves.

Además trata acerca del hacking cuando se refiere a la inutilización de programas, descifrado de claves.

Finalmente en sí, a toda infracción en el cual se vean inmiscuidos medios electrónicos ya sea un ordenador, una red, una tarjeta magnética, medios electrónicos en general, violación de seguridades tecnológicas, con la finalidad de apropiarse fraudulentamente de bienes de una tercera persona.

Artículo 231.- *Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.*

Con igual pena, será sanciona da la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

De igual manera el Fraude Informático Se encuentra regulado en el art. 231, al recordar que le trasfondo del fraude es el beneficio económico, este articulo trata sobre la trasferencia electrónica de activo patrimonial, que se equipara al Fraude Informático, en este caso, se da a conocer el ánimo de la persona que es el lucro, lo que le lleva a cometer el ilícito mediante la manipulación o modificación del funcionamiento de sistemas informáticos y lo que incluya ello, manifestándose claramente la modalidad de fraude efectuado por manipulación informática, cuyo fin es transferir o apropiarse de activos patrimoniales de otras personas.

Además de ello, se reprime de igual manera, a aquella persona que facilite sus datos con la única intención de percibir ilegalmente beneficios económicos para sí mismo o para una tercera persona.

Constitución de la República del Ecuador

En cuanto a la carta magna, garantiza el derecho a la protección de los datos e información de carácter personal.

Derechos de libertad

Art. 66.- *Se reconoce y garantizará a las personas:*

***19**. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.*

La constitución reconoce y garantiza que los datos de las personas, su información, son protegidos por el Estado. Es decir, que nadie puede disponer de ellos arbitrariamente.

Actualmente la información de una persona está contenida en una base de datos, así por ejemplo el Registro Civil lleva una base de datos con la información de una persona unificándose con otras bases como del Consejo Nacional Electoral, Las instituciones educativas entre otras, creando un cumulo de información de cada ciudadano. Dicha información puede ser requerida debidamente mediante los mecanismos legales, pero si es revelada ilegalmente por personas particulares o funcionarios públicos serán sancionados conforme el COIP lo establece.

Esta disposición puede relacionarse con el Fraude Informático, en el caso de que delincuente manipule un sistema informático con la intención de robar información ya sea datos personales, números de cuentas claves, para finalmente usarlos en beneficio propio o ajeno, afectando gravemente a la persona titular.

3.4 Legislación Comparada

3.4.1 Legislación Española

Dentro de la legislación de España, los delitos informáticos y específicamente el Fraude Informático se encuentra regulado en el *Código Penal Español referentes a Delitos Informáticos: Ley-Orgánica 10/1995, de 23 de Noviembre/ BOE número 281, de 24 de Noviembre de 1.995.*

En la ley española, el fraude es considerado como una modalidad de estafa por lo que se aplica los preceptos relativos a la penalidad de la estafa y agravaciones, esto por cuanto la finalidad de la estafa y del fraude son los mismos.

Siendo regulado en el art. 248 del Código Penal Español:

Artículo 248

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Al analizar se puede advertir que trata acerca de la estafa pero en el numeral 2 del artículo hace referencia a la estafa que se lo realiza por manipulación de medios informáticos transfiriendo activos patrimoniales provocando perjuicio económico al titular de dichos activos, observándose así que se cumplen los presupuestos para el fraude informático.

No obstante la Ley Orgánica 15/2003 de 25 de noviembre agrega en el numeral 2 del art. 248[53] los presupuestos del fraude informático que se lo trata como estafa, resultando así:

Artículo 248

[53] Artículo 248 redactado por el apartado sexagésimo primero del artículo único de la L.O. 5/2010, de 22 de junio, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 23 junio).Vigencia: 23 diciembre 2010

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

En este artículo modificado se puede apreciar que se consideran ya a los actos preparatorios del delito en sí, como lo es la fabricación, introducción o quien provee programas informáticos que se destinen a cometer el ilícito claramente, es más, que inclusive la posesión de dichos programas son considerados también como actos preparatorios y a la vez quienes se encuadren dentro de este presupuesto serán considerados como reos.

Luego refiere a quienes, sin ser titulares, utilicen medios electromagnéticos como una tarjeta de crédito o debido, o documentos emitidos por entidades financieras para que cuyo titular pueda utilizarlo en otro país y sea canjeado por dinero o como medio de pago, por ejemplo los cheques de viaje, produciendo un perjuicio patrimonial al titular o a un tercero.

La Ley Penal Española, considera a las defraudaciones patrimoniales por medios informáticos que se las puede realizar por dos formas, una de ellas por la manipulación deliberada de medios informáticos, por ejemplo transfiriendo activos de una cuenta bancaria sin autorización a otra a

beneficio suyo o de un tercero, y una segunda forma que es mediante la conducta ilícita y abusiva de documentos que contienen información de su titular y que dan acceso a los activos del mismo, por ejemplo la clonación de tarjetas.

La sanción del fraude informático se encuentra regulada en el art. 249.

Artículo 249

Los reos de estafa serán castigados con la pena de prisión de seis meses a cuatro años, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Se establece como sanción prisión que puede ir de seis meses a un año, todo dependerá del valor defraudado, el impacto económico causado al ofendido, si hubo o no una relación entre ellos, los medios empleados y las circunstancias en que se cometió el hecho delictivo.

3.4.2 Legislación Argentina

El Código Penal Argentino, tipifica y sanciona lo relacionado al fraude informático en su capítulo IV *Estafa y otras defraudaciones e*n los siguientes artículos:

Artículo 172. - *Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.*

Artículo 173.- *Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:*

15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.[54]

En la legislación argentina el Fraude Informático fue introducido en el año 2008 mediante una reforma, ubicándose en el art. 173 numeral 16, como una modalidad de defraudación, siendo esta característica el uso de medios tecnológicos, refiere a quien defraude a otra persona, es decir despoje, robe a otra persona ya sea mediante la manipulación informática o cualquier técnica que altere el funcionamiento correcto de un sistema informático, que no es más que la descripción en si del fraude informático.

Además en el numeral precedente, regula el skimming que es robo de información de tarjetas de crédito o de debido al momento de la transacción, con la finalidad de clonar dicha tarjeta y darle uso fraudulento posteriormente.

En esta legislación es reprimido el Fraude Informático con prisión de un mes a seis años

[54] Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008

3.5 Recomendaciones para evitar ser víctima de un delito informático

Para evitar ser víctima de un delito informático, en el ámbito laboral se recomienda:

- El aspirante al cargo de personal de sistemas informáticos de una empresa debe someterse a un examen psicosométrico, para evaluar alguna variable psicológica, que puede prevenir el ingreso de una persona con tendencias marcadas a la delincuencia informática.
- En los contratos de trabajo, incluir cláusulas especiales de confidencialidad con su respectiva penalidad, en donde se establezca claramente que el personal deberá guardar escrupulosamente los secretos técnicos que tenga por razón del cargo que vaya a desempeñar.
- Capacitaciones permanentes, para prevención de acciones negligentes o imprudenciales.
- Cambiar las claves o passwords con frecuencia, y establecerlas con un nivel de dificultad alto.

En el ámbito general, se recomienda:

- Ingresar a sitios web seguros
- No ingresar a la Deep web, puesto que es un sitio en donde los hackers están acechando a su posible víctima, pudiendo llegar a ocasionarle graves perjuicios al usuario.
- Al terminar de navegar, ya sea en un ordenador personal o de uso múltiple, borrar el historial de navegación.
- Al entrar a redes sociales, cuentas, correos o paginas donde tenga que ingresar con un nombre de usuario y password, no poner la opción “recordar contraseña” nunca, ya que por descuido propio podemos perder la pc y alguien más tener acceso a la misma, u otra posibilidad es el olvidar cerrar sesión en otro ordenador quedando a disposición y uso de cualquier otra persona.

- No abrir correos spam, porque pueden contener virus maliciosos para el sistema informático.
- No descargar programas o información de origen desconocido o dudoso, porque puede infectar de malware el ordenador.
- Al darle mantenimiento a la pc, hacerlo en un lugar de confianza porque personas inescrupulosas pueden hacer mal uso de la información entregada en el ordenador.
- Tener un programa antivirus instalado y actualizado con filtro anti-spam.
- Este tipo de recomendaciones puede ser aplicadas ya sea al ordenador, como a un smarthphone u otro medio tecnológico que se utilice para navegar en el internet.

Recomendaciones para evitar ser víctima de Fraude Informático y sus modalidades:

- Cuando vaya a realizar transacciones virtuales bancarias, realizarlo desde un ordenador personal, desde la página oficial de la entidad financiera, para estar seguros de que la página web es la correcta, esta ha de empezar con *https:* y antes de esto aparecerá un candado y el nombre del sitio al que desea acceder por ejemplo*: Banco Pichincha C.A. [EC] https://www.pichincha.com/portal/inicio.*
- No proporcionar datos personales, números de cuentas, claves de acceso si quien le está solicitando no se identifica debidamente o si lo hace desde un medio no idóneo, verifique la fuente de información.
- Las claves de acceso y usuarios son personales, en lo posible, no prestar este tipo de información a nadie.
- Cambiar constantemente las claves de acceso de cuentas bancarias.
- Si recibe un correo que al parecer es de un sitio confiable, no ingrese directamente desde el link que contiene el correo, escriba la dirección en el navegador.
- Revisar periódicamente sus cuentas y estados a fin de detectar oportunamente trasferencias o transacciones no autorizadas.

- Para lo que respecta al alcance de la mayoría de los usuarios la técnica más usada es la de la infección del archivo host (pharming local). Simplemente busque el archivo host en su sistema y elimine cualquier línea con direcciones IP excepto aquella que define a "localhost" como 127.0.0.1

- Si tiene acceso a su router verifique que el número IP del servidor DNS configurado en el router sea el que le ha designado su proveedor de Internet o el administrador del sistema.[55]

[55] MAULINI R., Mauro, *"¿Qué es el pharming? Tipos de pharming y alcance"*, e-securing.com. s.pág. Online. Internet. Consultado: 10 febrero 2015. Recuperado de: http://www.e-securing.com/novedad.aspx?id=45

CONCLUSIONES

- La revolución tecnológica, permitió al ser humano materializar sus conocimientos y su afán de innovar en grandes descubrimientos como lo es el ordenador, que en un principio fueron grandes maquinas, muy costosas, y que solo ciertas personas podían acceder a ellas, hoy en día, con el desarrollo de las tecnologías, un ordenador tiene dimensiones pequeñas, accesibles para la sociedad, de fácil manejo y muy utilitarias, tanto que a diario se las utiliza para las distintas actividades de la persona.
- El delito del fraude informático se lo vincula con la estafa, ya que la finalidad del delincuente es el beneficio económico para sí mismo o para un tercero, no obstante, se lo diferencia por el medio utilizado, pues esencialmente el fraude informático se lo realiza por medio de la informática, tecnología o sistemas informáticos, razón fundamental para crear un tipo penal independiente a la estafa, sin embargo, existen legislaciones que todavía regulan al fraude informático dentro de la estafa como la legislación española y la argentina, pero dejando estableciendo claramente que se trata del fraude.
- La Criminalidad informática actual, se oriente principalmente a los actos económicos, hechos delictivos que buscan atacar la economía ya sea de una persona natural o una persona jurídica, sin dejar de lado que existen delincuentes que a más de buscar el beneficio económico procuran al satisfacción personal al demostrar sus habilidades para burlar protecciones de seguridad a sistemas informáticos, lo hacen a manera de pasatiempo y por saciar su curiosidad, unos terceros lo hacen para obtener información confidencial que pueden ser de personas jurídicas de derecho privado como público, nacionales o extranjeros, cuya única finalidad es divulgar la información obtenida, creando inestabilidad e inseguridad en cuanto a la seguridad de los sistemas.
- La finalidad del delincuente informático variará según sean sus conocimientos, su preparación y sus intereses, así un hacker quien

entrará deliberadamente a un sistema sin autorización para obtener información a diferencia de un craker que lo único que le interesa es manipular el software, vulnerar sus seguridades, hacerlo operativo y accesible a cualquier persona sin necesidad de pagar por él.

- El bien jurídico protegido del delito informático siempre será la información a pesar de que algunos autores consideren que el bien jurídico protegido es la reserva, la intimidad, la propiedad. Estos son bienes jurídicos protegidos que se derivan de la información, puesto que de ahí parte la afectación de los demás bienes jurídicos.
- La tecnología puede ser utilizada como medio o como fin para el cometimiento de un hecho delictivo, así como medio se utiliza un ordenador para perpetrar el delito, por ejemplo utilizando una computadora se falsifica documentos. En tanto que como fin, se establece como blanco del delito el ordenador, los circuitos, colapsar un sistema, etc.
- A los delitos informáticos les caracteriza por ser considerados de cuello blanco, esto es, que quien comete el mismo no puede ser cualquier persona, tendrá que ser un individuo con cierta preparación o educación en tecnología, informática, sistemas computacionales, etc. Inclusive el perfil criminológico de estos delincuentes
- Hoy en día las modalidades de fraude más usuales son el phishing y pharming, que se lo realiza principalmente con miras a obtener información confidencial del usuario por medios fraudulentos como una página web falsa, cuya finalidad es usar dicha información para obtener beneficios económicos a favor del ciberdelincuente.
- La realidad en el Ecuador, sobre el Fraude Informático, y los delitos informáticos en general, es que crecen anualmente, a pesar de que se ha tratado de regular los delitos informáticos desde la Ley de Comercio Electrónico, Mensajes de Datos y Firmas, hasta el vigente Código Orgánico Integral Penal, se hace necesario una regulación especial vaya a la par con este fenómeno delictual, pues se trata del Derecho

Informático que a diferencia de otras ramas del derecho, está en constante cambio y evolución.

- La tecnología es muy importante para las actividades diarias, sean actividades investigativas, comunicacionales, comerciales, entretenimiento, entre otros, siendo importante brindar seguridad a quienes la utilizan diariamente, dicha seguridad se refleja en la seguridad jurídica que puede brindar cada país en sus legislaciones internas para combatir la vulneración a los derechos provenientes de la utilización de la informática.
- Ante todo, la primera seguridad a la que nos debemos los usuarios, es a utilizar la tecnología con cautela, con responsabilidad y prudencia, porque muchas veces los delitos se perpetran por la negligencia de la persona.
- Es importante recalcar que en la sociedad de la información, hacen falta profesionales de derecho expertos en Derecho Informático, o un grupo de trabajo con profesionales de Derecho y de Informática con equipos de última tecnología, trabajando colectivamente contra la delincuencia tecnológica.

BIBLIOGRAFÍA

- ACURIO DEL PINO, Santiago, "*Delitos Informáticos*", oas.org. Online. Internet.(http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf)
- CAPITANT, Henri, "*Vocabulario Jurídico*", Ediciones Depalma, Buenos Aires, 1961
- CASTRO, Luis, About en español. Online. Internet. (http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es Hacker.htm)
- Código Orgánico Integral Penal Ecuatoriano, Suplemento - Registro Oficial Nº 180, Quito, 2014
- Código Penal Argentino, Ley N^{o}. 11.179,
- Código Penal Español, Ley Orgánica N$^{o.}$ *281, 1995*.
- Constitución de la República del Ecuador, Registro Oficial N^{o} 449 ,Quito, 2008.
- Convenio sobre la ciberdelincuencia, Budapest, 2001
- CORREA Carlos y otros autores, "Derecho Informático", Editorial Depalma, Buenos Aires, 1987
- DAVARA Miguel Ángel*, "Derecho Informático*", Ed. Arzandi, España, 1993
- ENDARA MORENO Julio, "Archivo de Criminología Neuropsiquiatría y Disciplinas Conexas", 3ra. Ed, Vol. XXVII, Editorial Universitaria, Quito, 1990.
- ESTRADA CABRERA, Yamilka, RAMOS ÁLVAREZ Everardo Luis, (Noviembre 2011), *"El fraude informático. Consideraciones generales"*, Contribuciones a las Ciencias Sociales, Online. Internet. (http://www.eumed.net/rev/cccss/14/ecra.html)
- GÓMEZ PEREZ, Mariana, "*Criminalidad informática, un fenómeno de fin de siglo*", ecured.cu,(Cuba). Online Internet.(http://www.ecured.cu/index.php/Criminalidad_inform%C3%A1tica)
- GUERRERO María Fernanda y otros autores, "Penalización De La Criminalidad Informática", Ediciones J. Gustavo Ibañez, Bogotá, 1998

- HALL, Andrés, "*Tipos de delitos informáticos: Los tipos de delitos informáticos reconocidos por Naciones Unidas"*, forodeseguridad.com. Online. Internet. (http://www.forodeseguridad.com/artic/discipl/disc_4016.htm)
- HUERTA MIRANDA, Marcelo, (marzo 2002), "*Figuras delictivo-informáticos tipificadas en Chile*", Alfa-redi. Online. Internet. (http://www.alfa-redi-org/rdiarticulo.shtml?=433)
- JIJENA Renato, "La Protección Penal De La Intimidad Y El Delito Informático", Editorial Jurídica de Chile, Chile, 1992
- NUÑEZ PONCE, Julio, "*Derecho Informático*", Lima –Perú, 1996
- RAMIREZ LUNA, César, "*EL PERFIL CRIMINOLOGICO DEL DELINCUENTE INFORMATICO* ",derecho.usmp. Online. Internet.(http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf)
- REBOLLO DELGADO Luprecio, "Derechos Fundamentales Y Protección De Datos", Editorial Dykinson, Madrid, 2004
- SOLANO BARCELAS Orlando, "Manual De Informática Jurídica", Ediciones J. Gustavo Ibañez, Bogotá, 1997
- TELLEZ VAVALDEZ Julio, "Derecho Informatico",3ª. Ed, Editorial Mc Graw Hill, México, 2014
- VALLEJO, María Cristina, (Julio 2013), "*El sabotaje o daño informático*", Derecho ecuador. Online. Internet. (http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/el-sabotaje-o-dantildeo-informaacutetico)
- ZAMBRANO REYNA, Regina, "*Delitos Informáticos*", *cecs.espol.* s.pág. Online.Internet.(http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf)